



Configuring SonicOS for Microsoft Azure

Configuration Guide

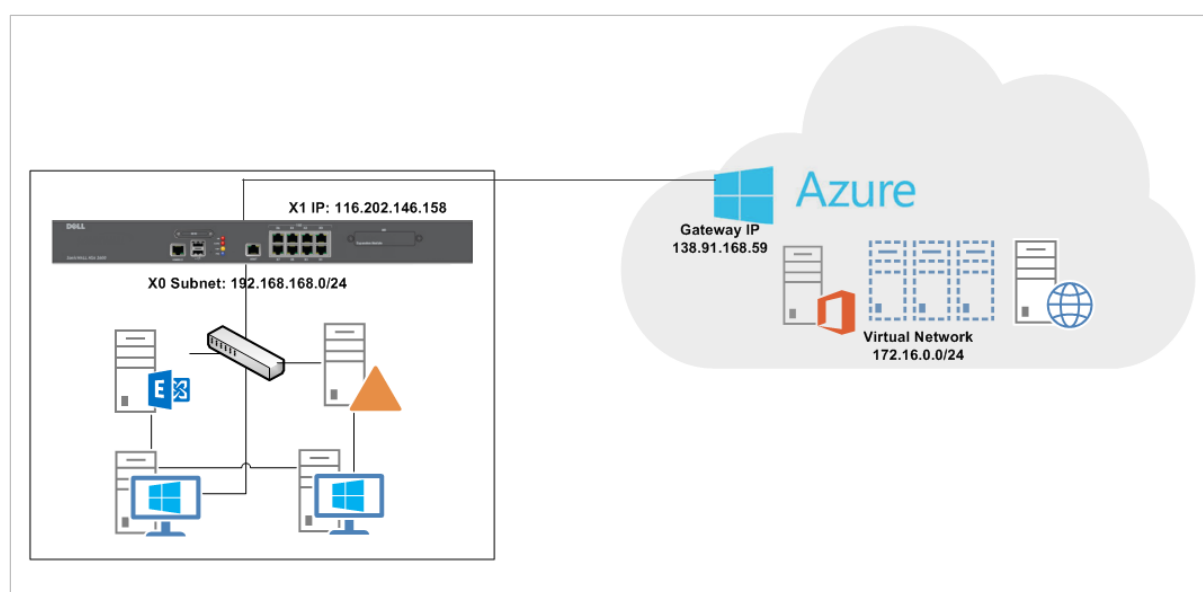
November 2015

Topics:

- [Purpose](#)
- [Deployment Considerations](#)
- [Supported Platforms](#)
- [Configuring a Policy-based VPN](#)
- [Configuring a Route-based VPN](#)

Purpose

This Configuration Guide details how to configure a policy-based or route-based VPN between Microsoft Azure and a Dell SonicWALL firewall running SonicOS. Azure is a cloud computing platform and infrastructure created by Microsoft. It is used for building, deploying, and managing applications and services through a global network of Microsoft managed datacenters. For SonicOS platforms, Azure provides site-to-site Virtual Private Network (VPN) connectivity between a Dell SonicWALL Next-Generation firewall and virtual networks hosted in the Azure cloud.



Deployment Considerations

Consider the following before deploying Microsoft Azure:

- The Azure Management Portal uses different terminology for VPNs than the SonicOS management interface, see the following for comparison:

VPN Terminology

Azure	SonicOS
Static Routing VPN	Site-to-Site VPN
Dynamic Routing VPN	Tunnel Interface VPN

- **Static Routing VPN** (Azure)/**Site-to-Site VPN** (SonicOS) are policy-based VPNs that allow users to specify a site-to-site network as part of a VPN policy, separate from a routing table lookup.
- **Dynamic Routing VPN** (Azure)/**Tunnel Interface VPN** (SonicOS) are route-based VPNs that can be used like an interface. This type of VPN can be configured with a route entry which is used to tunnel traffic as a part of the routing table lookup.

NOTE: Currently, only static routes are available for use with SonicOS because Azure does not support dynamic routing protocols such as BGP, OSPF, or RIP.

- For authentication, only Pre-shared Key (PSK) is currently supported, certificate based site-to-site VPNs are not yet supported.

Supported Platforms

Microsoft Azure is supported with the following Dell SonicWALL appliances:

- SuperMassive E10000 Series
- SuperMassive 9200 / 9400 / 9600
- E-Class NSA E5500 / E6500 / E7500 / E8500 / E8510
- NSA 2600 / 3600 / 4600 / 5600 / 6600
- NSA 220 / 220W / 240 / 250M / 250MW / 2400 / 2400MX / 3500 / 4500 / 5000
- TZ 100 / 100W / 105 / 105W / 200 / 200W / 205 / 205W / 210 / 210W / 215 / 215W
- TZ 300 / 300W / 400 / 400W / 500 / 500W / 600

Supported firmware

For the SuperMassive E10000 series, all approved versions of SonicOS support Microsoft Azure.

For platforms other than the SuperMassive E10000 Series, the following SonicOS firmware or hotfixes support the latest version of Microsoft Azure:

Supported firmware and associated platforms

Firmware or hotfix	Platforms supported
6.2.4.3 (December 2015)	TZ 300/300W, 400/400W, 500/500W, 600
6.2.3.1-19n--HF163571-1n	
6.2.2.3-20n support build	NSA 2600/3600/4600/5600/6600, SuperMassive 9200/9400/9600
5.9.1.1_39o--HF157568_2o	E-Class NSA E5500 / E6500 / E7500 / E8500 / E8510
5.9.1-39o--HF160565_3o	NSA 220/220W, 240, 250M/250MW, 2400, 2400MX, 3500, 4500, 5000
5.8.1.15	TZ 100/100W, 105/105W, 200/200W, 205/205W, 210/210W, 215/215W

Contact Support at <https://support.software.dell.com/manage-service-request> to obtain a hotfix or support build for your Dell SonicWALL firewall. Non-hotfix or support build firmware is available on MySonicWALL for your platform.

Configuring a Policy-based VPN

To configure a policy-based VPN between the Dell SonicWALL firewall and Microsoft Azure, complete the following tasks on each side of the deployment (Azure and SonicOS), then test the connectivity between them:

- [Azure Configuration Tasks](#)
- [SonicOS Configuration Tasks](#)
- [Testing the Connectivity](#)

Azure Configuration Tasks

The following sections describe creating a virtual network in the Microsoft Azure Management Portal.

- [Creating a Virtual Network](#)
- [Defining the SonicWALL Network](#)
- [Configuring a Virtual Network Address](#)
- [Creating a Virtual Network Gateway](#)
- [Managing Shared Keys](#)

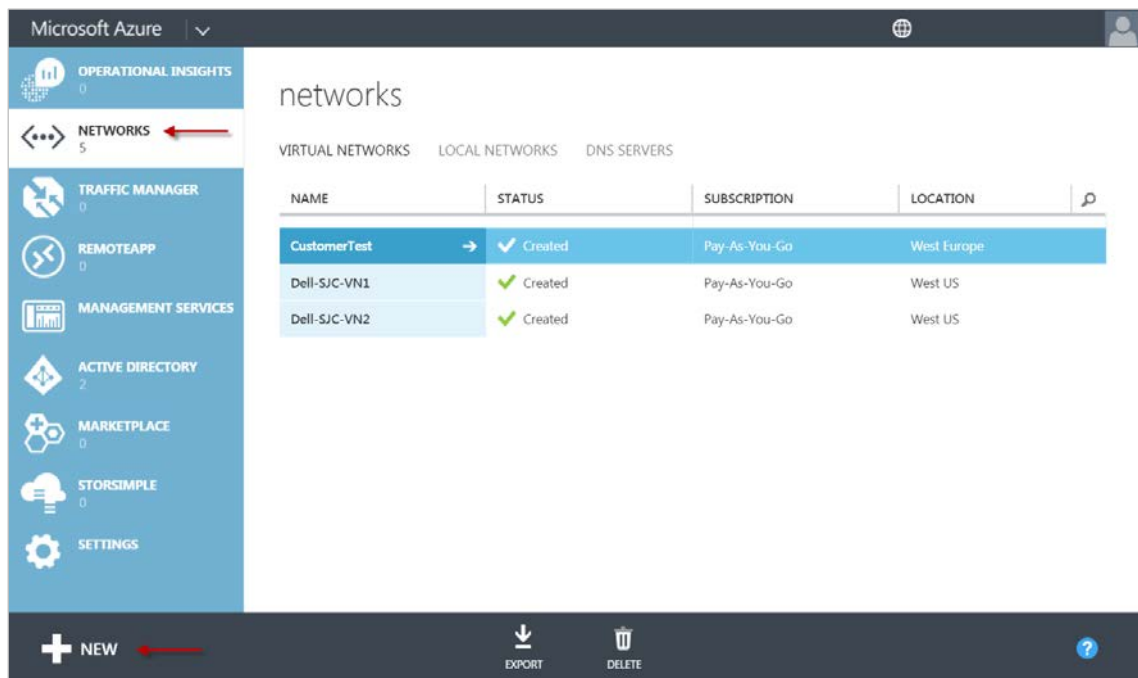
Creating a Virtual Network

To create a virtual network through the Microsoft Azure Management Portal, complete the following tasks:

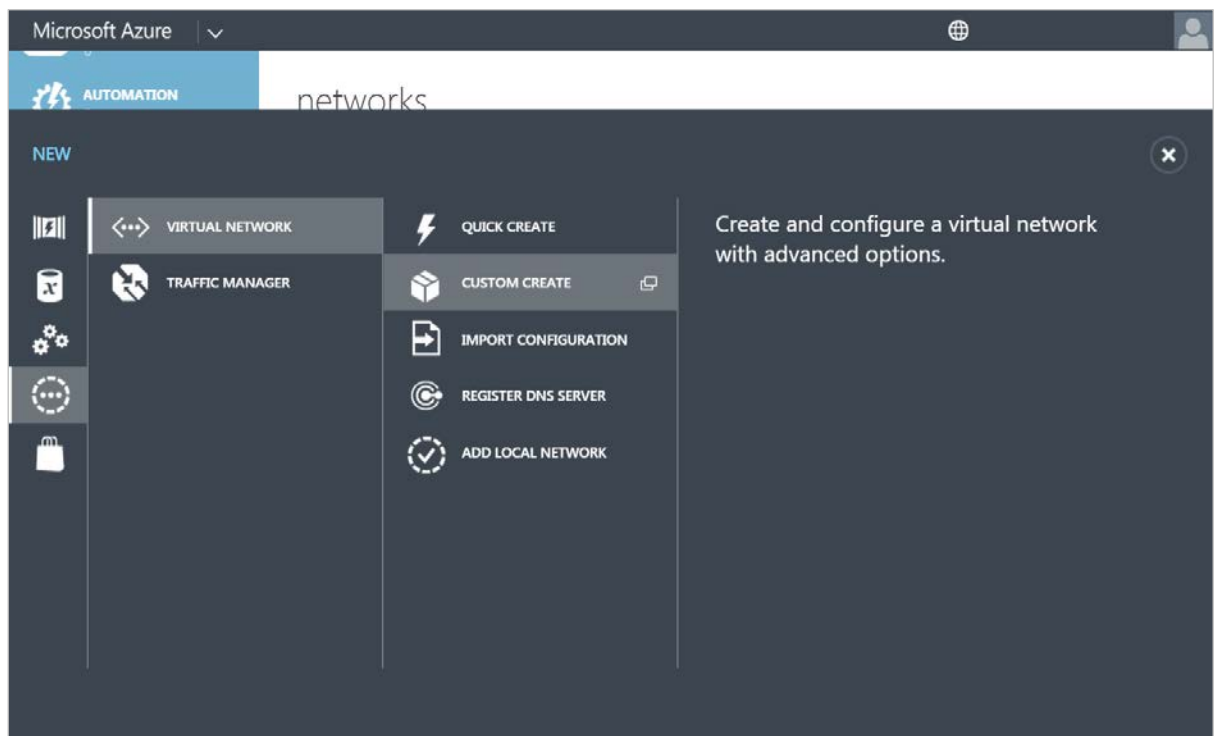
- 1 Log in to the [Microsoft Azure Management Portal](#).

- 2 In the left navigation menu, click **NETWORKS**.

The Networks dialog displays and shows a list of available virtual networks.



- 3 Click **NETWORKS > VIRTUAL NETWORK > CUSTOM CREATE**.



The **CREATE A VIRTUAL NETWORK** wizard displays:

- 4 On the Virtual Network Details dialog, enter the following information:
 - **NAME** - Name your virtual network. In this case, *TestVPN*.
 - **LOCATION** - Select a geographical location based on the options provided in the Azure portal.
- 5 Click the **Right Arrow** to continue to the next dialog.

Defining the SonicWALL Network

The DNS Servers and VPN Connectivity dialog displays. For more information about the settings on this dialog, refer to this MSN article on [DNS Servers and VPN Connectivity](#).

CREATE A VIRTUAL NETWORK

DNS Servers and VPN Connectivity

DNS SERVERS ?

ENTER NAME IP ADDRESS

POINT-TO-SITE CONNECTIVITY ?

☐ Configure a point-to-site VPN

SITE-TO-SITE CONNECTIVITY ?

☒ Configure a site-to-site VPN

☐ Use ExpressRoute

LOCAL NETWORK

Specify a New Local Network

- Azure-Network
- CusterNetwork
- Dell-Local
- Dell-SJC-Net
- Dell-SJC-Network
- TestVPN-LocalNet
- Specify a New Local Network

NETWORK PREVIEW

TestVPN GATEWAY VPN New Local

3 4

- 6 For **DNS SERVERS**, optionally fill in the **ENTER NAME** and **IP ADDRESS** fields. You can add DNS servers to your virtual network for name resolution. If you want to have name resolution between this virtual network and your on-premises network, you should specify the DNS servers that are used for your on-premises name resolution. You can also specify public DNS servers. If you do not specify a DNS server, name resolution is provided by Azure. The DNS server name and IP address entries are omitted for the purpose of this Configuration Guide.
- 7 Click **Configure a site-to-site VPN**.
- 8 Click the **LOCAL NETWORK** drop-down menu and either select a network (if it has been created already) or select **Specify a New Local Network**. The local network here is the network behind the Dell SonicWALL firewall.

- 9 Click the **right arrow** to proceed to the next dialog.

The **Site-to-Site Connectivity** dialog displays:

CREATE A VIRTUAL NETWORK

Site-to-Site Connectivity

NAME: TestVPN-LocalNet

VPN DEVICE IP ADDRESS: 208.140

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
192.168.37.0/24	192.168.37.0	/24 (256)	192.168.37.0 - 192.168.37.255

add address space

ADDRESS SPACE: /24 (256) /25 (128) /23 (512) /22 (1024)

NETWORK PREVIEW

TestVPN - GATEWAY - VPN - TestVPN-LocalNet

- 10 Enter the following information:

- **NAME** - Enter a name for your local network. This is the friendly name the Azure Virtual Network uses to refer to your on-premises local network. Entering a name does not configure any settings on your on-premises network.
- **VPN DEVICE IP ADDRESS** - This is the WAN IPv4 address of the Dell SonicWALL firewall. Enter the IP address of your local firewall. After you complete the Azure network configurations, you can configure your local firewall.

NOTE: The IP address of this firewall must be public-facing and cannot be located behind an NAT device.

- 11 Click **add address space** to add additional networks behind the Dell SonicWALL firewall. The **ADDRESS SPACE** (including **STARTING IP** and **CIDR**) is the internal network behind the Dell SonicWALL firewall. For more information about the settings on this dialog, refer to this [MSN article on Site-To-Site Connectivity](#).

- 12 Click the **right arrow** to proceed to the next dialog.

Configuring a Virtual Network Address

For more information about the settings on this dialog, refer to this MSN article titled [About Configuring a Virtual Network using the Management Portal](#).

After clicking the right arrow to the fourth dialog, the **Virtual Network Address Spaces** dialog displays:

CREATE A VIRTUAL NETWORK

Virtual Network Address Spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
40.0.0.0/16	40.0.0.0	/16 (65536)	40.0.0.0 - 40.0.255.255
SUBNETS			
Subnet-1	40.0.0.0	/28 (16)	40.0.0.0 - 40.0.31.255
add subnet add gateway subnet			
add address space			

NETWORK PREVIEW

TestVPN — GATEWAY — VPN — TestVPN-LocalNet

1 2 3 [Checkmark]

- 13 Click the **STARTING IP** drop-down menu, and then enter the network ID (private address range).
- 14 Click the **CIDR** drop-down menu, and then select the desired subnet bits.
- 15 Click **add gateway subnet**. The Gateway IP address is automatically populated based on the address space entered previously. Microsoft runs a gateway service to enable cross-premises connectivity. To this end, two IP addresses are required from the virtual network to enable routing between the physical premises and the cloud. A subnet with at least 29 bits in the routing prefix (/29 in CIDR notation) must be specified from which you can pick IP addresses for setting up routes.
- 16 Click the **Checkmark** to create your network.

After your virtual network is created, the **Management Portal > NETWORKS** dialog displays the **STATUS** as **Created**:

Microsoft Azure

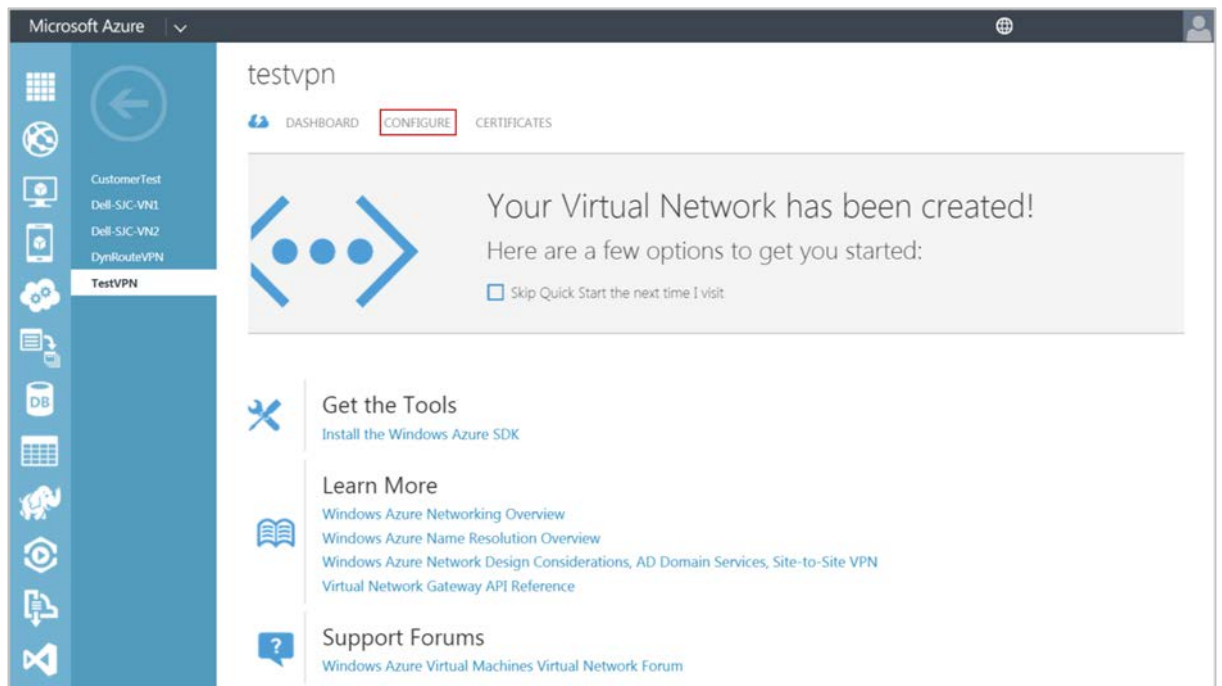
networks

VIRTUAL NETWORKS LOCAL NETWORKS DNS SERVERS

NAME	STATUS	SUBSCRIPTION	LOCATION
CustomerTest	Created	Pay-As-You-Go	West Europe
Dell-SJC-VN1	Created	Pay-As-You-Go	West US
Dell-SJC-VN2	Created	Pay-As-You-Go	West US
TestVPN	Created	Pay-As-You-Go	West US

At this point in the configuration, a virtual network is created in the cloud and a remote network is specified (the Dell SonicWALL network).

- 17 To view the configuration details, click the name of the virtual network (in this case *TestVPN*) in the NAME column.



- 18 On the TestVPN Quick Start dialog, click **CONFIGURE** to view the details. The TestVPN Configuration dialog appears.

Microsoft Azure | testvpn

DASHBOARD CONFIGURE CERTIFICATES

dns servers

ENTER NAME IP ADDRESS

point-to-site connectivity

CONNECTION ☐ Configure point-to-site connectivity

site-to-site connectivity

CONNECTION ☒ Connect to the local network

☐ Use ExpressRoute

LOCAL NETWORK TestVPN-LocalNet

virtual network address spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
40.0.0.0/16	40.0.0.0	/16 (65531)	40.0.0.4 - 40.0.255.254
SUBNETS			
Subnet-1	40.0.0.0	/24 (251)	40.0.0.4 - 40.0.0.254
Gateway	40.0.1.0	/29 (3)	40.0.1.4 - 40.0.1.6

add subnet add gateway subnet

add address space

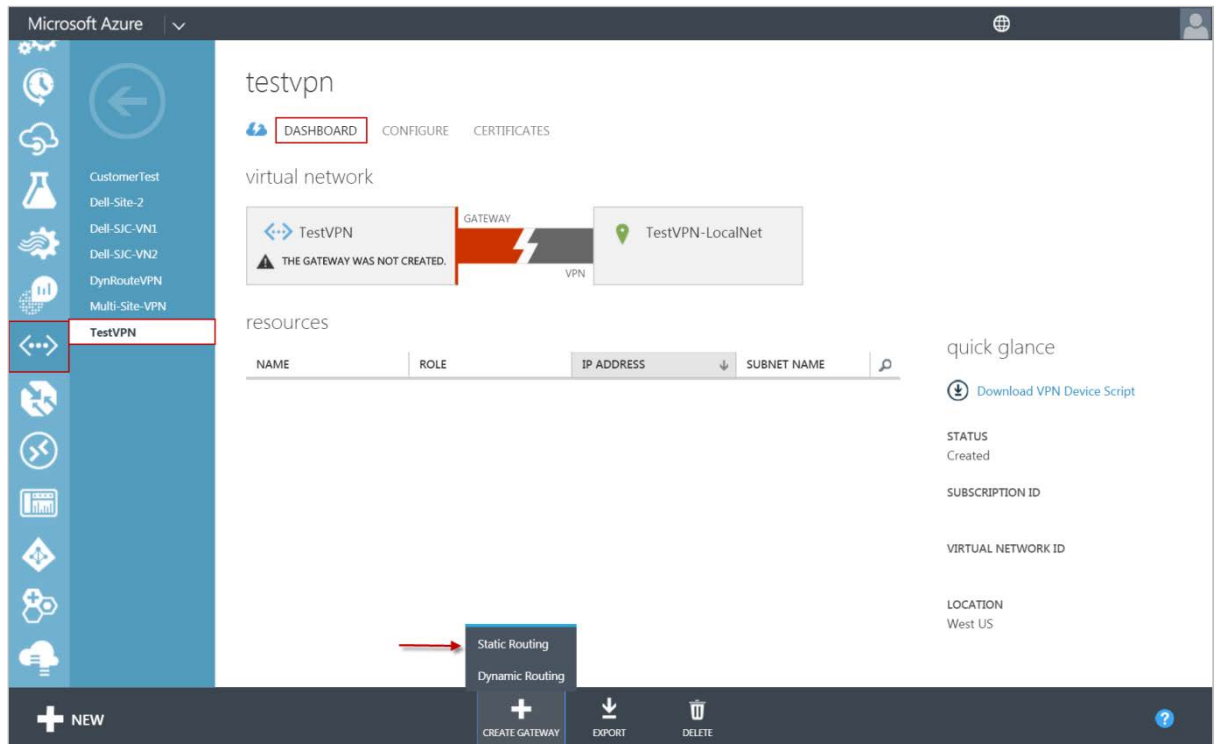
+ NEW

- 19 Add additional subnets and DNS servers as necessary.

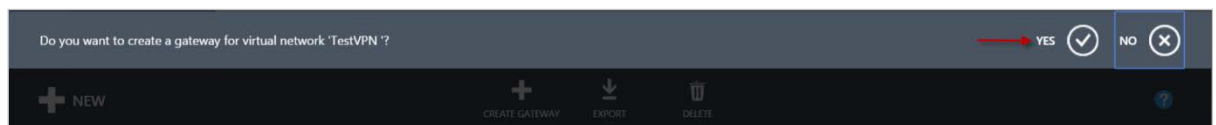
Creating a Virtual Network Gateway

20 On the TestVPN Quick Start dialog, click **DASHBOARD**.

At the bottom of the dialog, click **CREATE GATEWAY**, and then select **Static Routing**.



21 When prompted to confirm the gateway creation, click **YES**. Depending on your connection, it could take up to 15 minutes to create the gateway.



The updated TestVPN Quick Start dialog displays:

The screenshot shows the Azure portal interface for the TestVPN Quick Start dialog. The 'DASHBOARD' tab is active. The interface displays a diagram of a virtual network connected to a gateway and a local network. The 'GATEWAY IP ADDRESS' is highlighted as 40.118.208.208. The 'resources' table is empty. The 'quick glance' section shows the status as 'Created' and provides subscription and virtual network IDs.

The public facing IPv4 address is not generated until the gateway has been created. After the gateway is created, you should see the public facing IPv4 address of your virtual network under the **GATEWAY IP ADDRESS**. This IP address must be entered under the **VPN > Settings | VPN Policies Configure - IPsec Primary Gateway Name or Address** option in the Dell SonicWALL firewall.

IMPORTANT: The GATEWAY IP ADDRESS might change if the gateway is deleted and re-created.

Managing Shared Keys

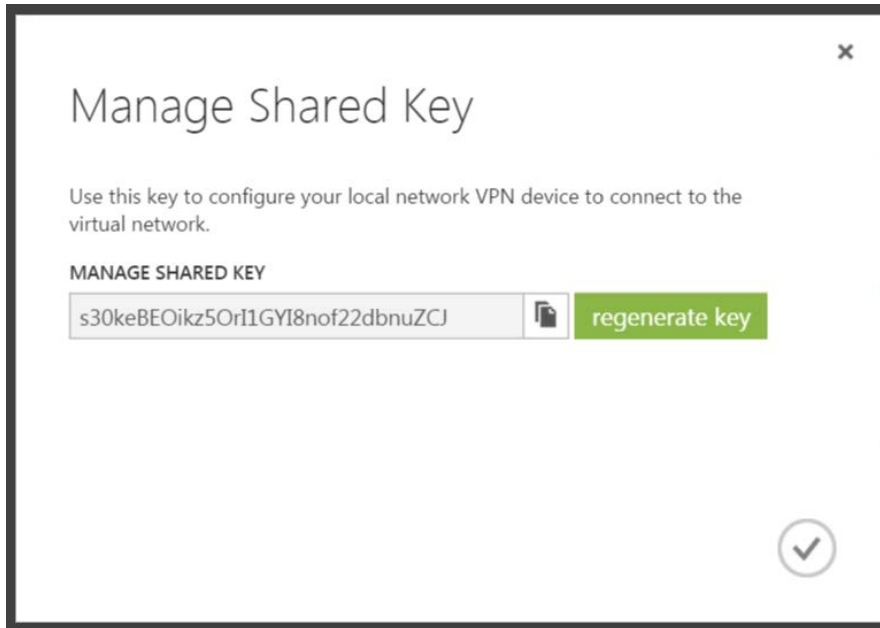
Use Shared Keys to configure your Dell SonicWALL firewall to connect to the Azure virtual network.

To obtain a Shared Key, complete the following steps:

- 22 Click **MANAGE KEY** at the bottom of the Azure Dashboard.




A pop-up dialog appears. This dialog includes an auto-generated shared key you can copy to connect the Microsoft Azure gateway and your Dell SonicWALL firewall.



- 23 Click the Copy icon next to the key to copy the shared key.

You can optionally click **regenerate key** should you decide to change the VPN preshared secret in the future.

 **CAUTION:** If you regenerate the key after using it to connect the firewall and the virtual network, the virtual network will lose connectivity with the local network until you reconfigure the firewall with the new key.

SonicOS Configuration Tasks

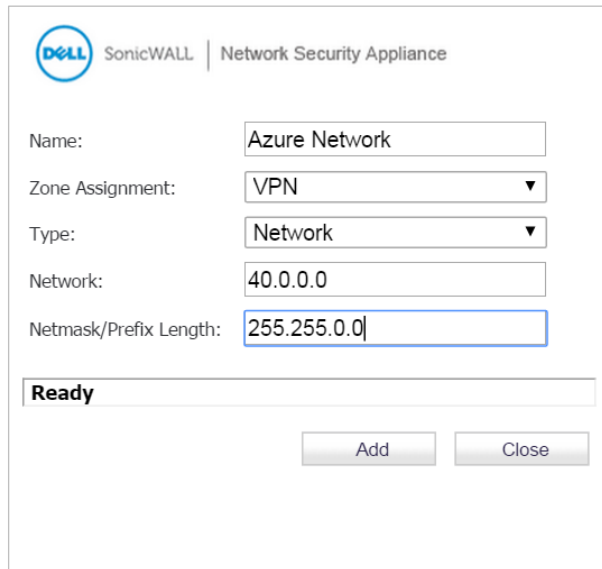
Use the SonicOS management interface of your Dell SonicWALL appliance to complete the following tasks:

- [Creating an Address Object for the Virtual Network](#)
- [Creating a Policy-Based VPN](#)

Creating an Address Object for the Virtual Network

- 1 Navigate to the **Network > Address Objects** dialog.
- 2 Click **Add...** to create a new Address Object.

The Add Address Object dialog displays:



NOTE: The information displayed in this dialog is for example only, and can vary depending on your network.

- 3 Enter the following information:
 - **Name** - Enter a name for the Address Object (*Azure Network* is used in this example)
 - **Zone Assignment** - Click the drop-down, and then select **VPN**.
 - **Type** - Click the drop-down, and then select **Network**.
 - **Network** - Enter the network IP address as shown in the [TestVPN](#) Quick Start dialog.
 - **Netmask/Prefix Length** - Enter the netmask.
- 4 Click **Add**.

Creating a Policy-Based VPN

To create a Policy-based VPN on the firewall:

- 5 Log in to the SonicOS management interface as an administrator.
- 6 Navigate to the **VPN > Settings** dialog.
- 7 Click **Add**.

The VPN Policy dialog displays:

The screenshot shows the SonicWALL Network Security Appliance VPN Policy dialog. The 'General' tab is active. The 'Security Policy' section includes: Policy Type (Site to Site), Authentication Method (IKE using Preshared Secret), Name (Azure), IPsec Primary Gateway Name or Address (40.118.208.208), and IPsec Secondary Gateway Name or Address (0.0.0.0). The 'IKE Authentication' section includes: Shared Secret (masked), Confirm Shared Secret (masked), Local IKE ID (IPv4 Address), Peer IKE ID (IPv4 Address), and a checked 'Mask Shared Secret' checkbox. At the bottom, there is a 'Ready' status bar and 'OK', 'Cancel', and 'Help' buttons.

8 Enter the following information:

- **Policy Type** - Select **Site to Site** from the drop-down menu.
- **Authentication Method** - select the **IKE using Preshared Secret** authentication method.
- **Name** - Enter a name for the policy (this example uses **Azure**).
- **IPsec Primary Gateway Name or Address** - Enter the **GATEWAY IP ADDRESS** displayed on the **Virtual Network TestVPN Dashboard** dialog of the Azure Management Portal. Refer to the [Creating a Virtual Network Gateway](#) section.
- **Shared Secret** - This is auto-generated by Azure. Copy it from the Azure Virtual Network dashboard, under **Manage Key**, and then enter it into this field. For more information, see [Managing Shared Keys](#).

9 Click the **Network** tab.

10 Click the **Choose local network from list** radio button, and then select the desired local network (This could vary depending on your network. The **X0 Subnet** is used in this example).

NOTE: This needs to be the same local network that was previously entered in the Azure Management Portal under the **Starting IP** text-field. Refer to [Defining the SonicWALL Network](#) to obtain this IP address.

- 11 Click **Choose destination network from list**, and then select the desired address object name, *Azure Network* in this example, from the drop-down menu.

The screenshot shows the SonicWALL Network Security Appliance configuration interface. The top navigation bar includes the SonicWALL logo and the text "SonicWALL | Network Security Appliance". Below this is a tabbed interface with four tabs: "General", "Network" (which is highlighted with a red border), "Proposals", and "Advanced".

Under the "Network" tab, there are two sections:

- Local Networks**: This section contains two radio buttons. The first, "Choose local network from list", is selected. To its right is a drop-down menu showing "X0 Subnet". The second radio button is "Any address".
- Remote Networks**: This section contains two radio buttons. The first, "Use this VPN Tunnel as default route for all Internet traffic", is unselected. The second, "Choose destination network from list", is selected. To its right is a drop-down menu showing "Azure Network".

At the bottom of the interface, there is a status bar that says "Ready". Below the status bar are three buttons: "OK", "Cancel", and "Help".

- 12 Click the **Proposals** tab.

- 13 Click the **Exchange** drop-down menu, and then select **Main Mode**.

Azure supports only Main Mode for static-routing site to site VPN. For more information about the Proposals supported in Azure, see the MSN article [About VPN Devices for Virtual Network](#).

SonicWALL | Network Security Appliance

General Network **Proposals** Advanced

IKE (Phase 1) Proposal

Exchange: Main Mode ▼

DH Group: Group 2 ▼

Encryption: AES-256 ▼

Authentication: SHA1 ▼

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP ▼

Encryption: AES-256 ▼

Authentication: SHA1 ▼

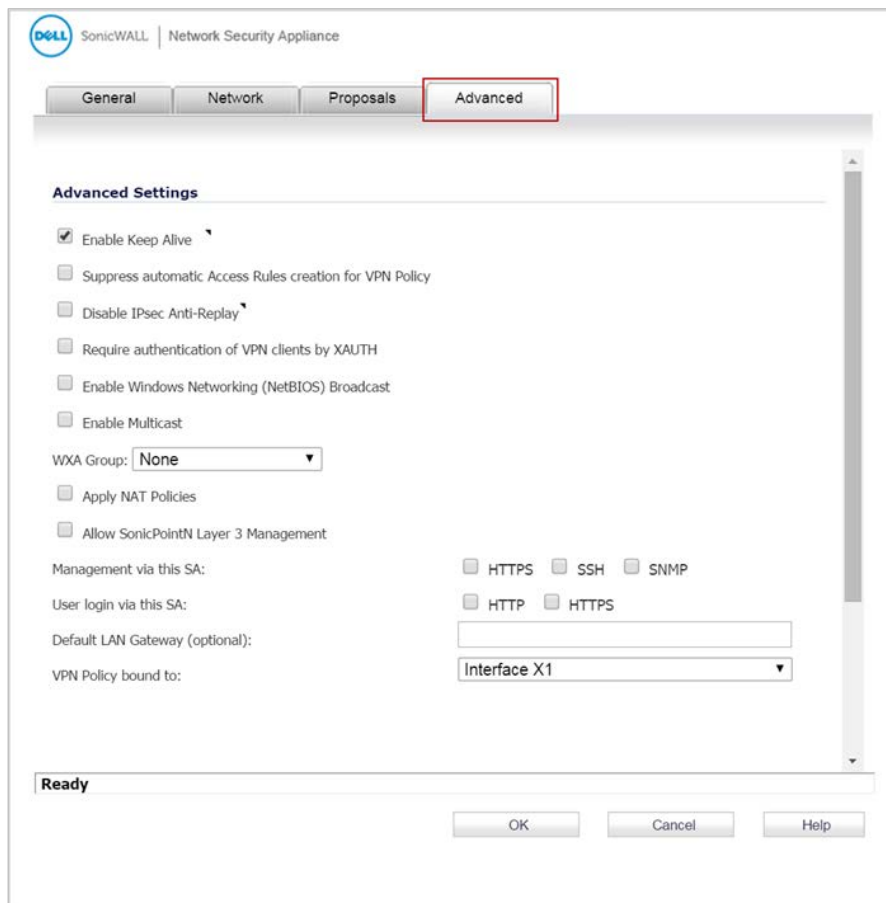
☐ Enable Perfect Forward Secrecy

Life Time (seconds): 3600

Ready

OK Cancel Help

14 Click the **Advanced** tab.



15 Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives allows for the automatic renegotiation of the tunnel without having to wait for the proposed Life Time to expire.

16 Click the **VPN Policy bound to** drop-down menu, and then select the appropriate interface (the WAN interface on the Dell SonicWALL firewall). For example: Interface X1.

17 Click **OK**.

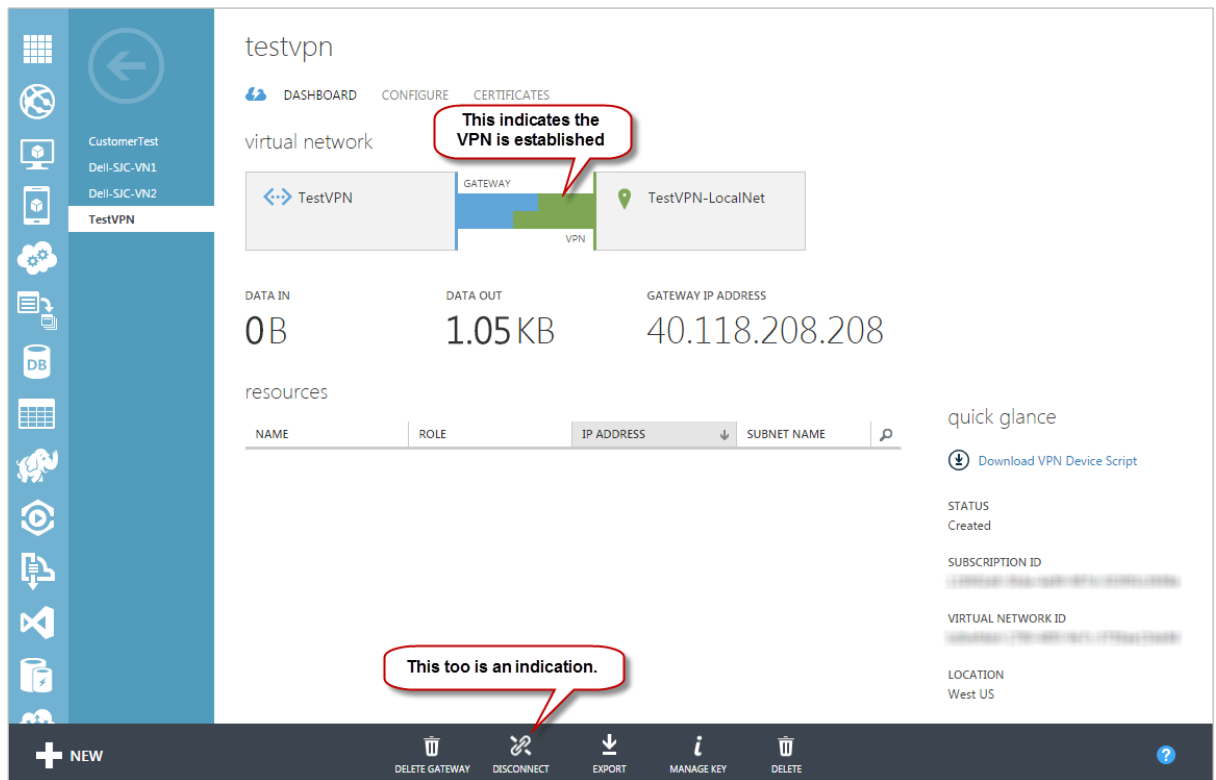
Testing the Connectivity

The SonicWALL firewall automatically initiates the VPN connection and keeps it alive when **Keep Alive** is enabled.

To test the connectivity from Azure:

- 1 Go to the Azure Management Portal, and navigate to **Networks**.
- 2 Click the virtual network and go to its **Dashboard** dialog.
- 3 Click **CONNECT** to initiate the VPN connection from the Azure gateway.

After a brief wait, the VPN tunnel shows as connected in the Azure Management Portal. After the tunnel is established, the portal appears as follows:



To test traffic flow from the Dell SonicWALL side to the Azure cloud, complete either of the following:

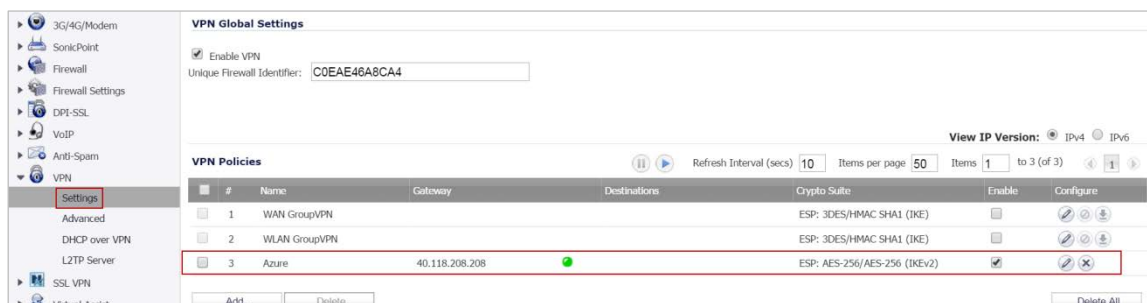
- Try to establish an RDP connection to a VM in the cloud on port 3389 from a host behind the Dell SonicWALL firewall.
- Try to ping a VM in the cloud from a host behind the Dell SonicWALL firewall.

NOTE: By default, a Virtual Machine (VM) in the Azure cloud has inbound ICMP blocked by the Windows firewall and needs to be enabled using this command: `netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any dir=in action=allow`

To test the connectivity from SonicOS:

- 1 Log in to the SonicOS management interface, and navigate to the VPN > Settings dialog.

In the VPN Policies table, the VPN shows as connected:



Configuring a Route-based VPN

To configure a route-based VPN between the Dell SonicWALL firewall and Microsoft Azure, complete the following tasks on each side of the deployment (Azure and SonicOS), then test the connectivity between them:

- [Azure Configuration Tasks](#)
- [SonicOS Configuration Tasks](#)
- [Testing the Connectivity](#)

Azure Configuration Tasks

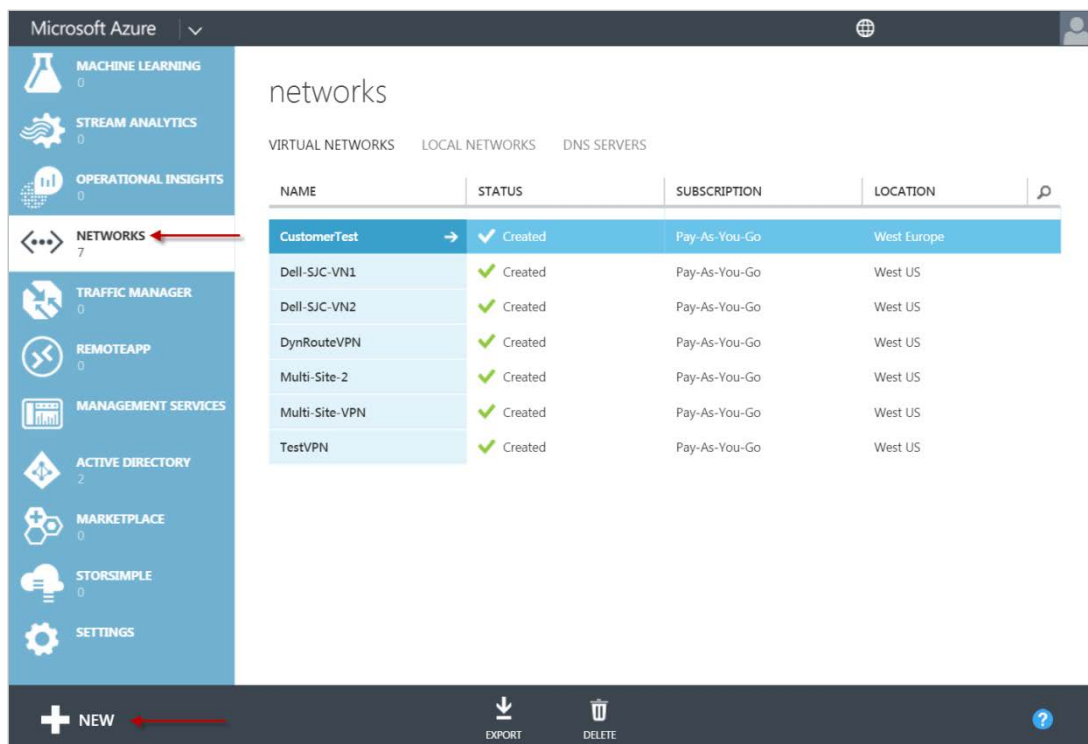
The following sections describe creating a virtual network in the Microsoft Azure Management Portal:

- [Creating a Virtual Network](#)
- [Defining the SonicWALL Network](#)
- [Configuring a Virtual Network Address](#)
- [Creating a Virtual Network Gateway](#)
- [Managing Shared Keys](#)

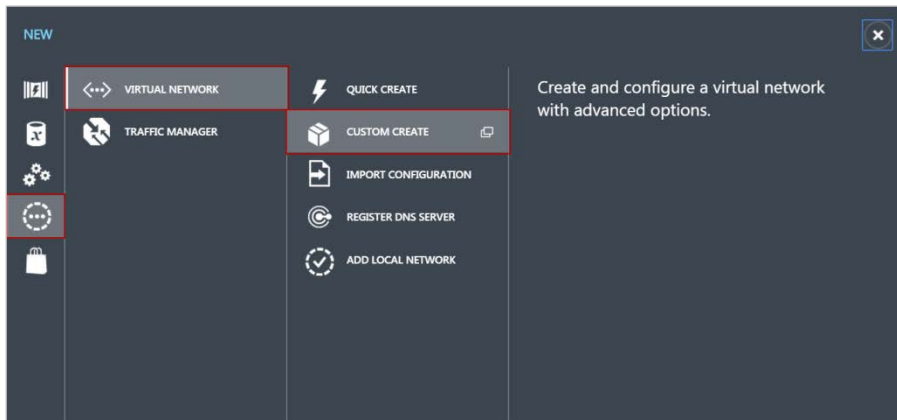
Creating a Virtual Network

To create a virtual network through the Microsoft Azure Management Portal:

- 1 Log in to the Microsoft [Azure Management Portal](#).
- 2 In the left navigation menu, click **NETWORKS** to show a list of available networks:



- 3 In the bottom left corner of the dialog, click **NEW**.
- 4 Click **NETWORKS > VIRTUAL NETWORK > CUSTOM CREATE**.



The Create a Virtual Network wizard displays:

A screenshot of the 'CREATE A VIRTUAL NETWORK' wizard in the Azure portal, specifically the 'Virtual Network Details' step. The form has two main sections: 'NAME' and 'LOCATION'. The 'NAME' field contains the text 'DynRouteVPN'. The 'LOCATION' dropdown menu is set to 'West US'. Below these fields is a 'NETWORK PREVIEW' section showing a small icon and the text 'DynRouteVPN'. At the bottom right, there is a right-pointing arrow button and a progress indicator showing '2' out of '3' steps.

- 5 On the Virtual Network Details dialog, enter the following information:
 - **NAME** - Name your virtual network. In this case, *DynRouteVPN*.
 - **LOCATION** - Select a geographical location based on the options provided in the Azure portal.
- 6 Click the **right arrow** to continue to the next dialog.

Defining the SonicWALL Network

For more information about the settings on this dialog, refer to this MSN article on [DNS Servers and VPN Connectivity](#).

The DNS Servers and VPN Connectivity dialog displays:

- 7 For **DNS SERVERS**, optionally fill in the **ENTER NAME** and **IP ADDRESS** fields. You can add DNS servers to your virtual network for name resolution. If you want to have name resolution between this virtual network and your on-premises network, you should specify the DNS servers that are used for your on-premises name resolution. You can also specify public DNS servers. If you do not specify a DNS server, name resolution is provided by Azure. The DNS server name and IP address entries are omitted for the purpose of this Configuration Guide.
- 8 Click **Configure site-to-site VPN**.
- 9 Click the **LOCAL NETWORK** drop-down menu and either select a network (if it has been created already) or select **Specify a New Local Network**. The Local network would be the network behind the Dell SonicWALL firewall.
- 10 Click the **right arrow** to proceed to the next dialog.

The Site-to-Site Connectivity dialog displays:

CREATE A VIRTUAL NETWORK

Site-to-Site Connectivity

NAME
Dell-SJC-Net

VPN DEVICE IP ADDRESS
208.11.1.40

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
172.16.0.0/16	172.16.0.0	/16 (65536)	172.16.0.0 - 172.16.255.255
ADDRESS SPACE	STARTING IP	/16 (65536)	USABLE ADDRESS RANGE

add address space

NETWORK PREVIEW

DynRouteVPN

GATEWAY

VPN

Dell-SJC-Net

1 2 4

11 Enter the following information:

- **NAME** - Enter a name for your local network. This is the friendly name the Azure Virtual Network uses to refer to your on-premises local network. Entering a name does not configure any settings on your on-premises network.
- **VPN DEVICE IP ADDRESS** - This is the WAN IPv4 address of the Dell SonicWALL firewall. Enter the IP address of your local firewall. After you complete the Azure network configurations, you can configure your local firewall.

NOTE: The IP address of this firewall must be public-facing and cannot be located behind an NAT device.

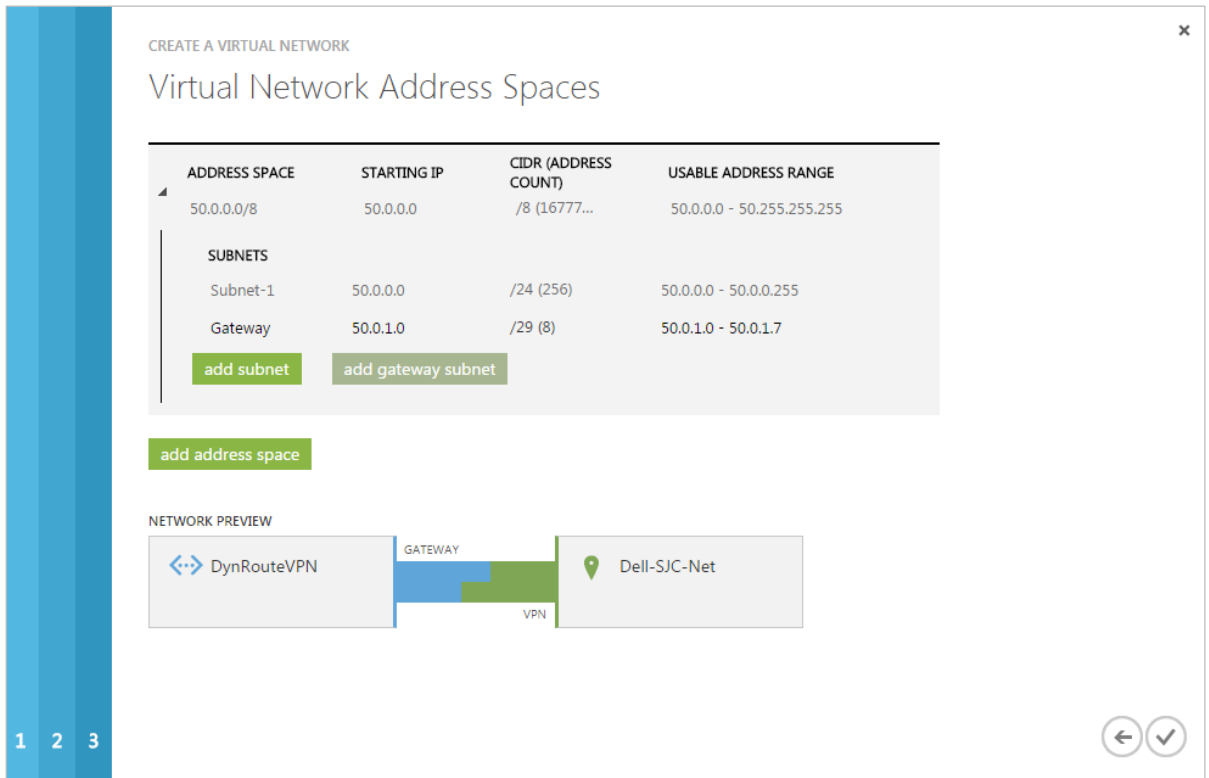
12 Click **add address space** to add additional networks behind the Dell SonicWALL firewall. The **ADDRESS SPACE** (including **STARTING IP** and **CIDR**) is the internal network behind the Dell SonicWALL firewall. For more information about the settings on this dialog, refer to this MSN article on [Site-To-Site Connectivity](#).

13 Click the **right arrow** to proceed to the next dialog.

Configuring a Virtual Network Address

For more information about the settings on this dialog, refer to this MSN article titled [About Configuring a Virtual Network using the Management Portal](#).

The **Virtual Network Address Spaces** dialog displays showing the protected network behind the Azure virtual gateway:



ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
50.0.0.0/8	50.0.0.0	/8 (16777...	50.0.0.0 - 50.255.255.255
SUBNETS			
Subnet-1	50.0.0.0	/24 (256)	50.0.0.0 - 50.0.0.255
Gateway	50.0.1.0	/29 (8)	50.0.1.0 - 50.0.1.7

add subnet add gateway subnet

add address space

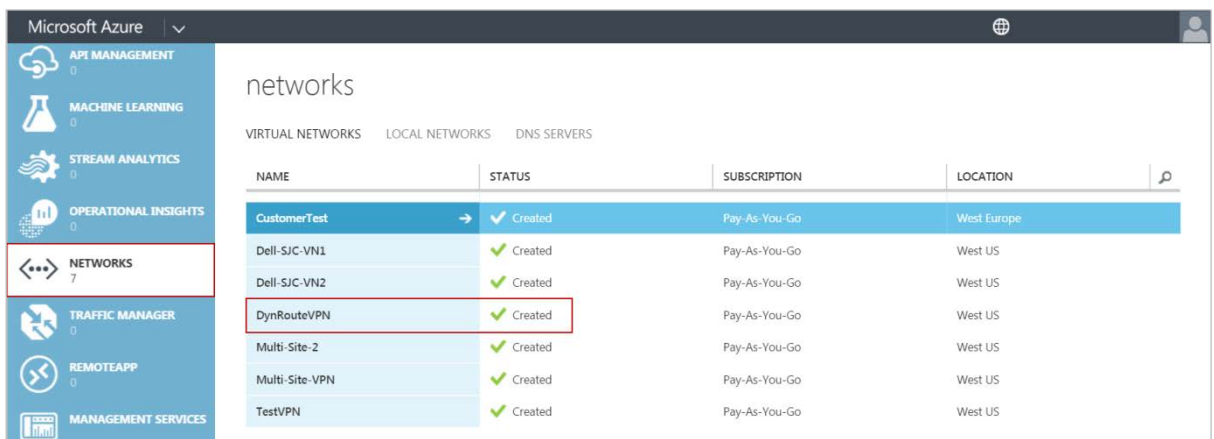
NETWORK PREVIEW

DynRouteVPN GATEWAY Dell-SJC-Net VPN

1 2 3

- 14 Click the **STARTING IP** drop-down menu, and then enter the network ID (private address range).
- 15 Click the **CIDR** drop-down menu, and then select the desired subnet bit.
- 16 Click **add gateway subnet**. The Gateway IP address is automatically populated based on the address space entered previously. Microsoft runs a gateway service to enable cross-premises connectivity. To this end, two IP addresses are required from the virtual network to enable routing between the physical premises and the cloud. A subnet with at least 29 bits in the routing prefix (/29 in CIDR notation) must be specified from which you can pick IP addresses for setting up routes.
- 17 Click the **checkmark** to create your network.

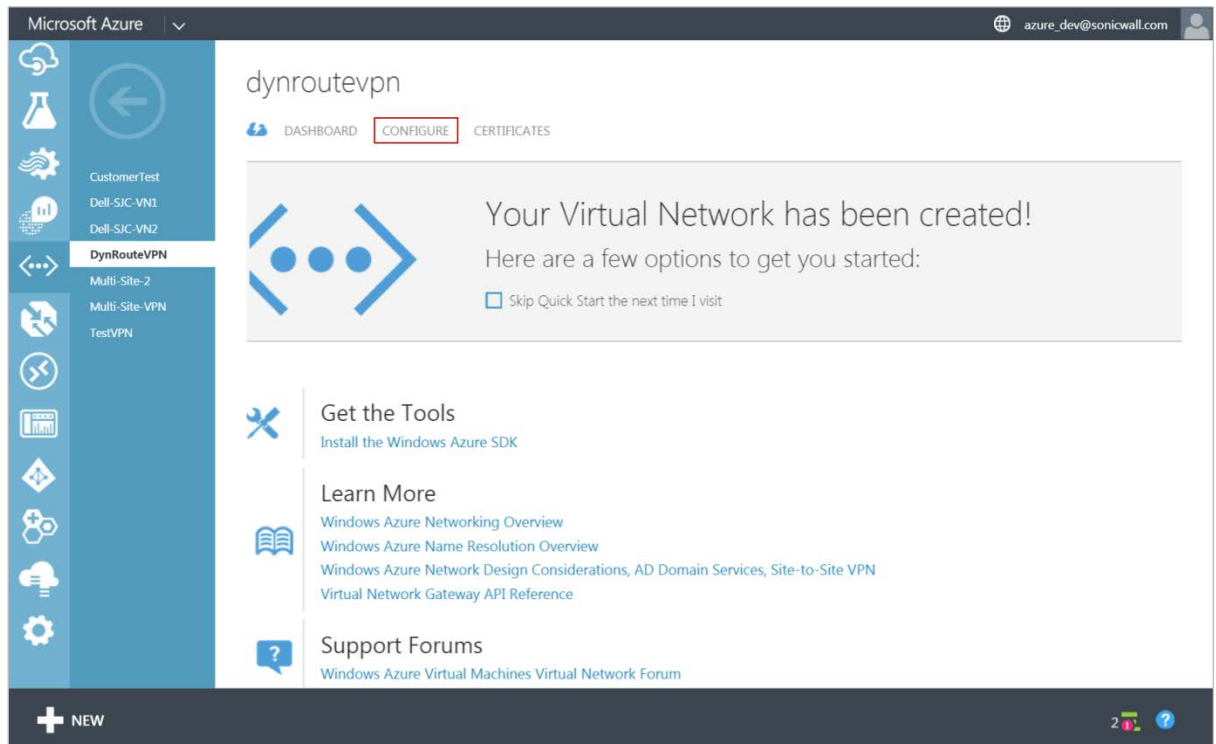
After your virtual network is created, the **Management Portal > NETWORKS** dialog displays the **STATUS** as **Created**.



NAME	STATUS	SUBSCRIPTION	LOCATION
CustomerTest	✓ Created	Pay-As-You-Go	West Europe
Dell-SJC-VN1	✓ Created	Pay-As-You-Go	West US
Dell-SJC-VN2	✓ Created	Pay-As-You-Go	West US
DynRouteVPN	✓ Created	Pay-As-You-Go	West US
Multi-Site-2	✓ Created	Pay-As-You-Go	West US
Multi-Site-VPN	✓ Created	Pay-As-You-Go	West US
TestVPN	✓ Created	Pay-As-You-Go	West US

At this point in the configuration, a virtual network is created in the cloud and a remote network is specified (as the on premise network).

- 18 To view the configuration details, click the name of the virtual network (in this case **DynRoutevpn**) in the **NAME** column.



- 19 On the DynRouteVPN Quick Start dialog, click **CONFIGURE** to view the details. The DynRouteVPN Configuration dialog appears.

dynroutevpn

DASHBOARD CONFIGURE CERTIFICATES

dns servers

ENTER NAME IP ADDRESS

point-to-site connectivity

CONNECTION ☐ Configure point-to-site connectivity

site-to-site connectivity

CONNECTION ☒ Connect to the local network

☐ Use ExpressRoute

LOCAL NETWORK Dell-SJC-Vnet

virtual network address spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
50.0.0.0/8	50.0.0.0	/8 (16777...	50.0.0.4 - 50.255.255.254
SUBNETS			
Subnet-1	50.0.0.0	/24 (251)	50.0.0.4 - 50.0.0.254
Gateway	50.0.1.0	/29 (3)	50.0.1.4 - 50.0.1.6

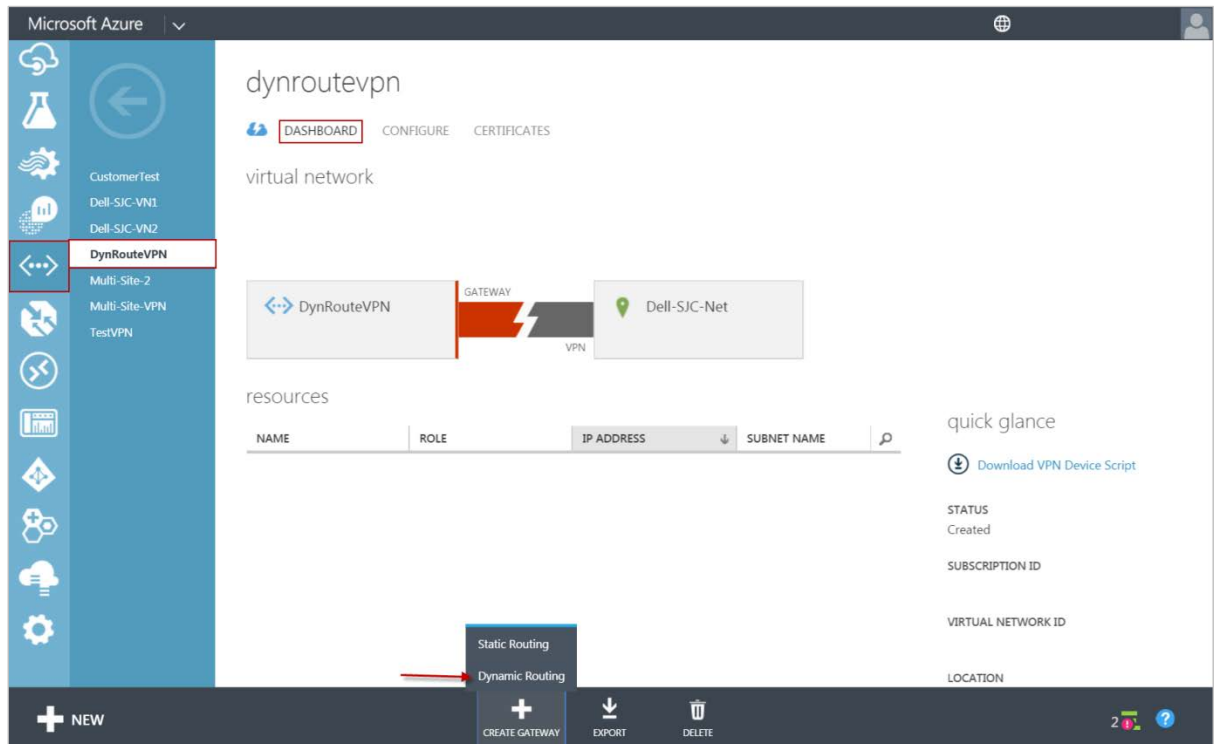
add subnet add gateway subnet

add address space

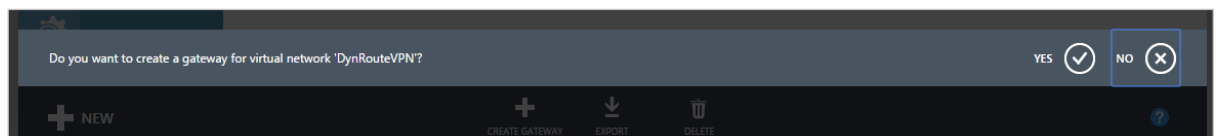
- 20 Add additional subnets or DNS servers if necessary.

Creating a Virtual Network Gateway

- 21 On the DynRouteVPN Quick Start dialog, click **DASHBOARD**.
- 22 At the bottom of the dialog, click **CREATE GATEWAY**, and then select **Dynamic Routing**.



- 23 When prompted to confirm the gateway creation, click **YES**. Depending on your connection, it could take up to 15 minutes to create the gateway.



The updated DynRouteVPN Quick Start dialog displays:

The screenshot shows the Azure portal interface for the DynRouteVPN configuration. The left sidebar contains navigation icons and a list of resources including 'CustomerTest', 'Dell-SJC-VN1', 'Dell-SJC-VN2', 'DynRouteVPN', and 'TestVPN'. The main content area displays the 'dynroutevpn' configuration page with tabs for 'DASHBOARD', 'CONFIGURE', and 'CERTIFICATES'. The 'virtual network' section shows a diagram with a 'DynRouteVPN' gateway connected to a 'Dell-SJC-Net' virtual network. The 'GATEWAY IP ADDRESS' is highlighted as '40.112.184.251'. Below this, the 'resources' table is shown with columns for NAME, ROLE, IP ADDRESS, and SUBNET NAME. The 'quick glance' section on the right provides a summary of the configuration, including STATUS (Created), SUBSCRIPTION ID, VIRTUAL NETWORK ID, LOCATION (West US), and GATEWAY TYPE (Dynamic Routing). At the bottom, a navigation bar contains buttons for 'DELETE GATEWAY', 'DISCONNECT', 'EXPORT', 'MANAGE KEY', and 'DELETE'. A red arrow points to the 'DISCONNECT' button.

The public facing IPv4 address is not generated until the gateway has been created. After the gateway is created, you should see the public facing IPv4 address of your virtual network under the **GATEWAY IP ADDRESS**. This IP address must be entered under the **IPsec Primary Gateway Name or Address** in the Dell SonicWALL firewall.

NOTE: The **GATEWAY IP ADDRESS** might change if the gateway is deleted and re-created.

Managing Shared Keys

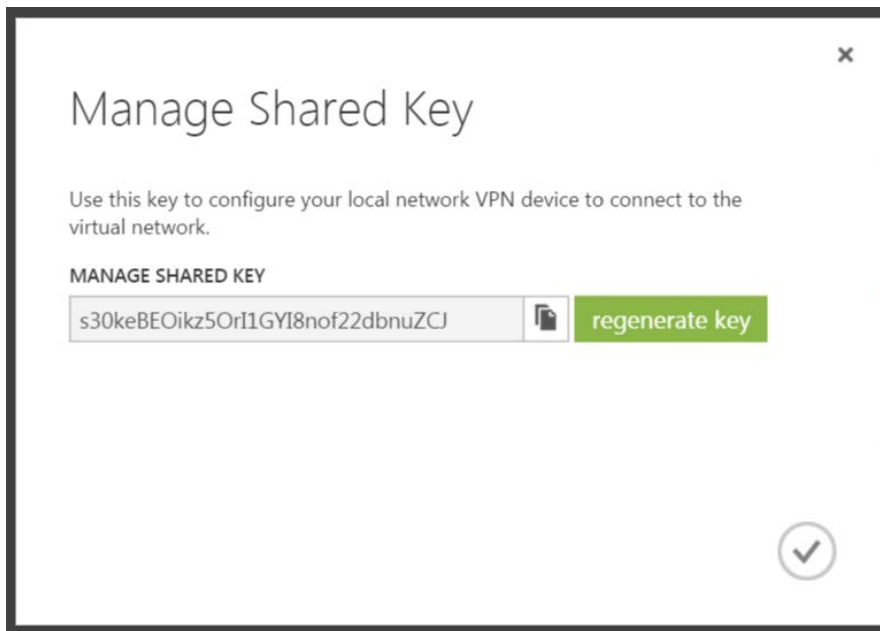
Use Shared Keys to configure your local network VPN device to connect to the virtual network.

To obtain a Shared Key, complete the following steps:

- 24 Click **Manage Key** at the bottom of the Azure Dashboard.



A pop-up dialog appears. This dialog includes an auto-generated shared key you can copy to connect the Microsoft Azure gateway and your Dell SonicWALL firewall.



- 25 Click the **Copy** icon next to the key to copy the shared key.

You can optionally click **regenerate key** should you decide to change the VPN preshared secret in the future.



CAUTION: If you regenerate the key after using it to connect the firewall and the virtual network, the virtual network loses connectivity with the local network until you reconfigure the firewall with the new key.

SonicOS Configuration Tasks

Complete the following in the SonicOS management interface of your Dell SonicWALL appliance:

- [Creating a Tunnel Interface VPN](#)
- [Creating an Address Object for the Virtual Network](#)
- [Creating a Static Route Policy](#)

Creating a Tunnel Interface VPN

- 1 Log in to the SonicOS management interface as an administrator.
- 2 Navigate to the **VPN > Settings** dialog.
- 3 Click **Add**.

The VPN Policy dialog displays:

SonicWALL | Network Security Appliance

General | Proposals | Advanced

Security Policy

Policy Type: Tunnel Interface ▼

Authentication Method: IKE using Preshared Secret ▼

Name: Azure

IPsec Primary Gateway Name or Address: 40.112.184.251

IKE Authentication

Shared Secret:

Confirm Shared Secret: ☒ Mask Shared Secret

Local IKE ID: IPv4 Address ▼

Peer IKE ID: IPv4 Address ▼

Ready

OK Cancel Help

4 Enter the following information:

- **Policy Type** - Select **Tunnel Interface** from the drop-down menu.
- **Authentication Method** - select **IKE using Preshared Secret**.
- **Name** - Enter a name for the policy (*Azure* is used in this example).
- **IPsec Primary Gateway Name or Address** - Enter the **GATEWAY IP ADDRESS** displayed on the **Virtual Network TestVPN Dashboard** dialog of the Azure Management Portal. For more information, see the [DynRouteVPN Quick Start](#) dialog.
- **Shared Secret** - This is auto-generated by Azure. Copy it from the Azure Virtual Network dashboard, under **Manage Key**, and then enter it into this field. For more information, see [Managing Shared Keys](#).

5 Click the **Proposals** tab.

6 Click the **Exchange** drop-down menu, and then select **IKEv2 Mode**.

Azure supports only IKEv2 Mode for route-based site-to-site VPN. For more information about the settings on this dialog, refer to this MSN article titled [About VPN Devices for Virtual Network](#).

The screenshot shows the 'Proposals' tab of the SonicWALL Network Security Appliance configuration interface. The 'General' tab is selected, and the 'Proposals' tab is highlighted with a red box. The 'Advanced' tab is also visible. The 'IKE (Phase 1) Proposal' section contains the following settings: Exchange: IKEv2 Mode, DH Group: Group 2, Encryption: AES-256, Authentication: SHA1, and Life Time (seconds): 28800. The 'Ipssec (Phase 2) Proposal' section contains the following settings: Protocol: ESP, Encryption: AES-256, Authentication: SHA1, and Life Time (seconds): 3600. There is an unchecked checkbox for 'Enable Perfect Forward Security'. At the bottom, there is a 'Ready' status bar and three buttons: OK, Cancel, and Help.

SonicWALL | Network Security Appliance

General | Proposals | Advanced

IKE (Phase 1) Proposal

Exchange: IKEv2 Mode
DH Group: Group 2
Encryption: AES-256
Authentication: SHA1
Life Time (seconds): 28800

Ipssec (Phase 2) Proposal

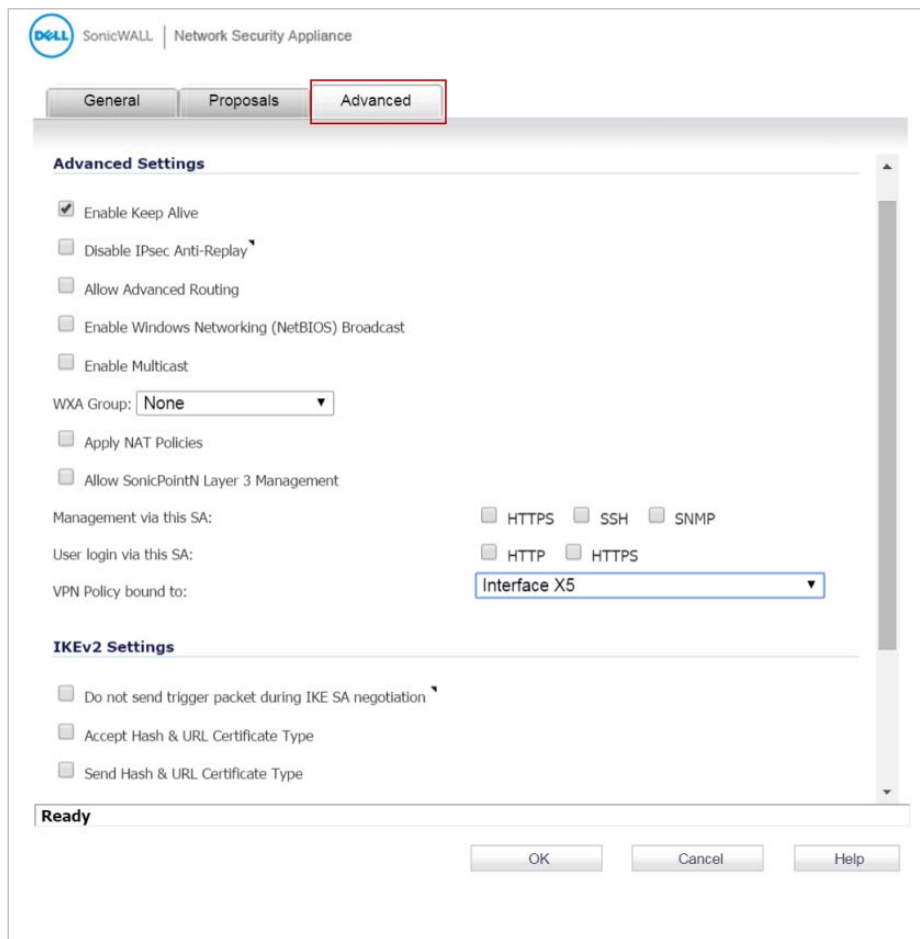
Protocol: ESP
Encryption: AES-256
Authentication: SHA1
☐ Enable Perfect Forward Security
Life Time (seconds): 3600

Ready

OK Cancel Help

- 7 Click the **Advanced** tab.
- 8 Enable Keep Alive by checking **Enable Keep Alive**.
- 9 Click the **VPN Policy bound** to drop-down menu, and then select a WAN interface. For example, *Interface X5*.

10 Click OK.



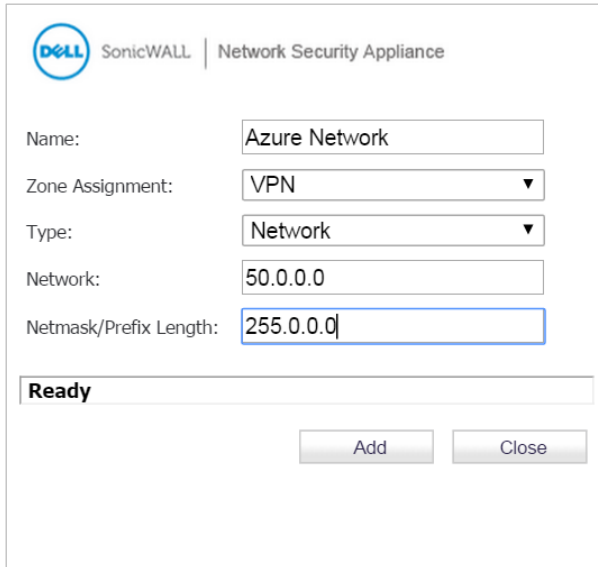
- 11 Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives allows for the automatic renegotiation of the tunnel without having to wait for the proposed Life Time to expire.
- 12 Click the **VPN Policy bound to** drop-down menu, and then select the appropriate interface (the WAN interface on the Dell SonicWALL firewall). For example: Interface X1.
- 13 Click OK.

Creating an Address Object for the Virtual Network

14 Navigate to the **Network > Address Objects** dialog.

15 Click **Add** to create a new Address Object.

The **Add Address Object** dialog displays:



The screenshot shows the 'Add Address Object' dialog in the SonicWALL Network Security Appliance interface. The dialog has a header with the Dell SonicWALL logo and the text 'Network Security Appliance'. Below the header, there are five input fields: 'Name' with the value 'Azure Network', 'Zone Assignment' with a dropdown menu showing 'VPN', 'Type' with a dropdown menu showing 'Network', 'Network' with the value '50.0.0.0', and 'Netmask/Prefix Length' with the value '255.0.0.0'. At the bottom of the dialog, there is a 'Ready' status bar and two buttons: 'Add' and 'Close'.

NOTE: The information displayed in this dialog is for example only, and can vary depending on your network.

16 Enter the following information:

- **Name** - Enter a name for the Address Object (*Azure Network* is used in this example)
- **Zone Assignment** - Click the drop-down, and then select **VPN**.
- **Type** - Click the drop-down, and then select **Network**.
- **Network** - Enter the network IP address as shown in the [Configuring a Virtual Network Address](#) section.
- **Netmask/Prefix Length** - Enter the netmask.

17 Click **Add**.

Creating a Static Route Policy

To create a static route policy, complete the following steps:

- 18 Navigate to the **Network > Routing** dialog.
- 19 Click **Add** to create a new Route Policy.

The **Add Route Policy** dialog displays:

SonicWALL | Network Security Appliance

General

Route Policy Settings

Source: X0 Subnet ▼

Destination: Azure Network ▼

Service: Any ▼

Gateway: 0.0.0.0 ▼

Interface: Azure ▼

Metric: 1

Comment:

☒ Disable route when the interface is disconnected

WXA Group: None ▼

☒ Auto-add Access Rules

Probe: None ▼

☐ Disable route when probe succeeds

☐ Probe default state is UP

Ready

OK Cancel Help

- 20 Configure **Source** to the same on-premise network you configured in the [Site-to-Site Connectivity](#) dialog.

NOTE: The information displayed in this screenshot is for example only, and could vary depending on your network.

- 21 Select **Disable route when the interface is disconnected**.
- 22 Select **Auto-add Access Rules**.
- 23 Click **OK**.

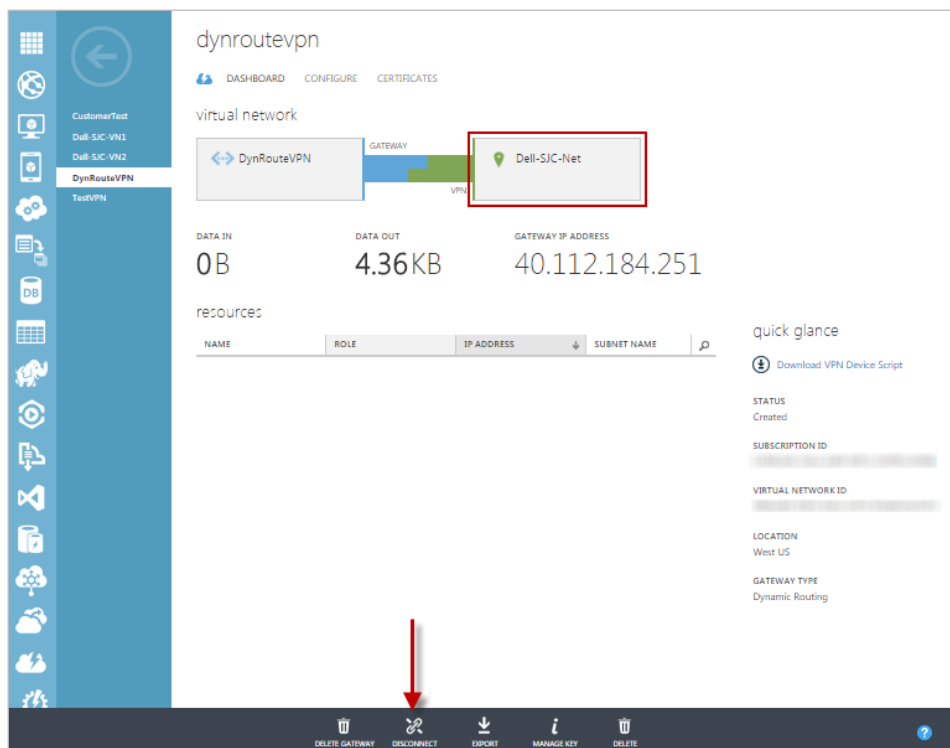
Testing the Connectivity

With the configurations completed on both sides, you can now initiate the VPN connection.

To test the connectivity from Azure:

- 1 Go to the Azure Management Portal, navigate to **NETWORKS**, and then click on your virtual network to go to its **Dashboard** dialog.
- 2 Because you enabled **Keep Alive**, the tunnel should be up at this stage. If not, click **CONNECT** to initiate the tunnel set up from the Azure gateway.

After a brief wait, the VPN tunnel shows as connected in the Azure Management Portal. After the tunnel is established, the portal appears as follows:



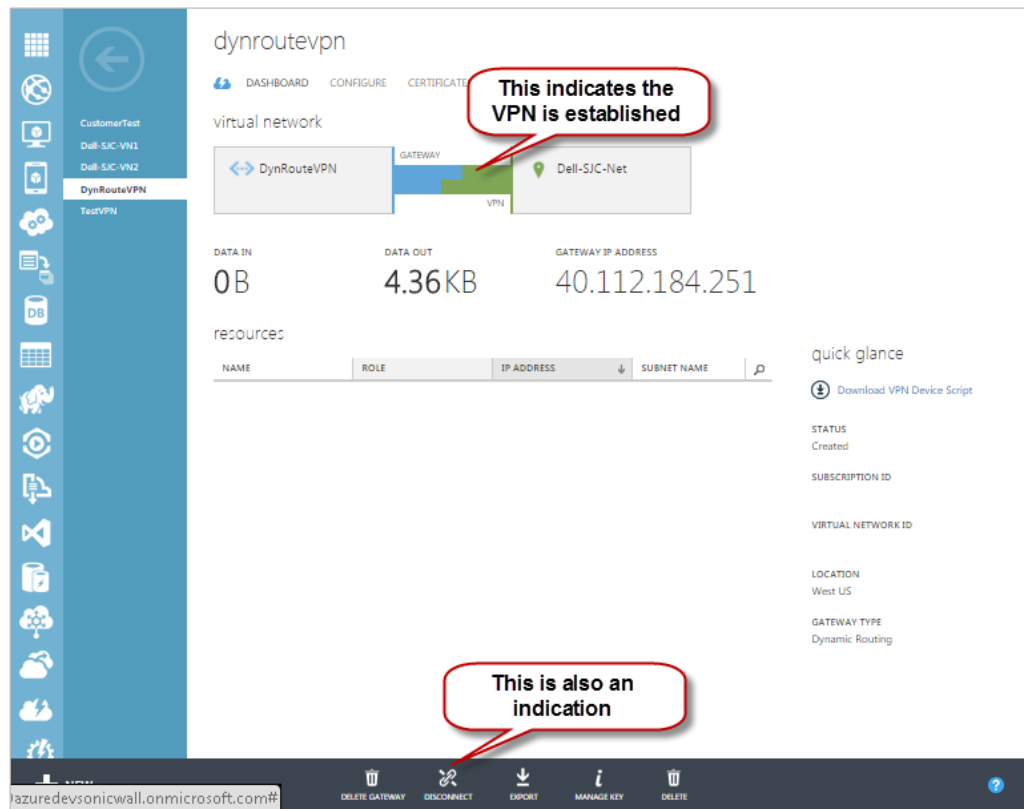
To test the connectivity from SonicOS:

- 1 Log in to the SonicOS management interface, and navigate to the **VPN > Settings** dialog.

In the VPN Policies table, the VPN shows as connected:



It might take a while for the VPN tunnel to show as connected in the Azure Management Portal. After the tunnel is established, the portal appears like this:



- 2 To test traffic flow from the SonicOS side to the Azure cloud, complete either of the following:
 - Try to establish an RDP connection to a Virtual Machine (VM) in the cloud on port 3389 from a host behind the Dell SonicWALL firewall.
 - Try to ping a VM in the cloud from a host behind the Dell SonicWALL firewall.

NOTE: By default, a VM in the Azure cloud has the inbound ICMP blocked by Windows Firewall and needs to be enabled in Windows using this command: `netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any dir=in action=allow`

© 2015 Dell Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Dell Inc.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Patents

For more information, go to <http://software.dell.com/legal/patents.aspx>.

Trademarks

Dell, the Dell logo, and SonicWALL are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend



CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.



IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 11/5/2015

232-002268-00 Rev C